Paul Curtis

I wish to include a brief professional history. I have been employed for 35 years in Information Technology—21 years specifically in Information Security--at companies, large and small, that have impact around the world. It is through that experience that I have become educated in the exceptionally high risk of mistakes, abuse and misuse of "digital media and technology in threat detection".

Artificial intelligence and machine learning rely heavily on the private companies and their employees that design, code, implement, manage and utilize the technology. Without extensive vetting, validation, removal of personal bias, tuning, oversight, cyber security controls and protections, this technology has an extremely high "false-positive" rate.

The negative impact of "false-positives" on innocent people can be staggering. The individuals who are identified as threats have a high probability of being visited by law enforcements officers with pistols, rifles and, in those circumstances deemed as life threatening, armored personnel carriers. And then begins the long, tenuous, costly legal proceedings.

In addition, artificial intelligence and machine learning have no judicial oversite nor do they have any due-process components associated with them.

What controls are in place to keep these tremendously powerful tools and processes from being weaponized by hackers, estranged or ex-spouses, or in extreme cases an opposing political party or bureaucrat?

While no one wants another heinous crime committed and innocent people hurt or killed, freedom-loving people have a God given, Constitutionally protected right to use social media--public and private forums--to discuss ideas, express their concerns, air grievances and criticize the government without fear of reprisal from an automated monitoring tool that is controlled by a person, group, government or company that does not share their opinion.

What part of freedom of speech are we willing to destroy by allowing technology to categorize good speech from bad?